CLAIMS

What is claimed is:

1. A method of providing access to a resource for one or more users, said method comprising:

receiving a request to issue authorization data for a user based on access rights associated with the user, said access rights including an expression identifying the resource by a resource name and by at least one property associated with the resource to conditionally define access to the resource; and

responsive to the received request, issuing the authorization data.

2. The method of claim 1, wherein receiving the request comprises receiving the request from an application program, and wherein issuing the authorization data comprises issuing the authorization data to the application program.

3. The method of claim 1, wherein receiving the request comprises receiving the request from a computing device, and wherein issuing the authorization data comprises issuing the authorization data to the computing device.

4. The method of claim 1, wherein receiving the request and issuing the authorization data occur over a secure sockets layer.

5. The method of claim 1, wherein receiving the request and issuing the authorization data occur over a network such as the Internet.

6. The method of claim 1, further comprising creating the authorization data in response to the received request.

7. The method of claim 6, further comprising encrypting the created authorization data.

8. The method of claim 6, further comprising:

generating a signature based on the created authorization data; and

including the generated signature and an expiration date with the created authorization data.

9. The method of claim 1, further comprising:

receiving the authorization data from an application program;

retrieving validation information from the received authorization data;

evaluating the retrieved validation information; and

sending a response indicating the validation status of the received authorization data responsive to said evaluating the retrieved validation information.

10. The method of claim 1, wherein one or more computer-readable media have computer-executable instructions for performing the method of claim 1.

11. A method for validating authorization data to provide access to a resource for one or more users, said method comprising:

receiving authorization data associated with one of the users, said authorization data including an expression identifying a resource by a resource name and by a property associated with the resource;

retrieving validation information from the received authorization data;

evaluating the retrieved validation information to determine a validation status of the received authorization data; and

sending a response indicating the determined validation status responsive to said evaluating the retrieved validation information.

12. The method of claim 11, further comprising evaluating the expression to identify the resource.

13. The method of claim 12, wherein evaluating the expression comprises extracting a target scope from the received authorization data, said extracted target scope identifying the resource.

14. The method of claim 11, wherein receiving the authorization data comprises receiving a data packet according to the Simple Object Access Protocol (SOAP), and further comprising extracting the authorization data from the received data packet.

15. The method of claim 11, wherein receiving the authorization data occurs over a secure sockets layer.

16. The method of claim 11, wherein receiving the authorization data occurs over a network such as the Internet.

17. The method of claim 11, further comprising decrypting the received authorization data.

18. The method of claim 11, wherein receiving the authorization data comprises receiving the authorization data from an application program, and further comprising:

receiving an identifier from the application program;

extracting another identifier from the received authorization data; and

comparing the received identifier with the extracted identifier to determine the validity of the received authorization data.

19. The method of claim 11, wherein retrieving the validation information comprises retrieving a signature from the received authorization data.

20. The method of claim 19, wherein evaluating the retrieved validation information comprises determining that the retrieved signature is invalid, and wherein sending the response comprises sending a response indicating the invalidity of the received authorization data.

21. The method of claim 11, wherein retrieving the validation information comprises retrieving an expiration date from the received authorization data, and wherein evaluating the retrieved validation information comprises comparing the retrieved expiration date to a current time stamp to determine if the received authorization data has expired.

22. The method of claim 21, wherein the received authorization data has been determined to be expired, and further comprising sending a response indicating the invalidity of the received authorization data.

23. The method of claim 11, wherein one or more computer-readable media have computer-executable instructions for performing the method recited in claim 11.

24. One or more computer-readable media having computer-executable components to control access to a resource by one or more users, said components comprising:

an interface component adapted to receive authorization data, said authorization data including an expression identifying a resource by a resource name and by a property associated with the resource;

a parser component adapted to retrieve validation information from the received authorization data; and

a validation component adapted to evaluate the retrieved validation information, wherein the interface component is further adapted to send a response indicating the validation status of the received authorization data responsive to said evaluating the retrieved validation information.

25. The computer-readable media of claim 24, wherein the interface component is further adapted to receive a request to issue the authorization data for a user based on access rights associated with the user.

26. The computer-readable media of claim 25, further comprising an authorization component adapted to issue the requested authorization data responsive to the request received by the interface component.

27. The computer-readable media of claim 24, further comprising a scope component to evaluate the expression to identify the resource.

28. An authorization system comprising:

a memory area for storing authorization data for use in accessing a resource, said authorization data including an expression identifying the resource by a resource name and by at least one property associated with the resource; and

a processor configured to execute computer-executable instructions for validating the authorization data to provide access to the resource.

29. The system of claim 28, wherein the processor is further configured to execute computer-executable instructions for issuing the authorization data for a user based on access rights associated with the user.

30. The system of claim 28, wherein the processor is further configured to execute computer-executable instructions for evaluating the expression to identify the resource.

31. The system of claim 28, wherein the authorization data comprises a token.

32. A computer-readable medium having stored thereon a data structure defining access by a user to a resource, said resource having one or more properties, said data structure comprising:

a header field representing validation information, said validation information including a signature and an expiration date;

a source field representing an identity of the user; and

a claim field specifying the resource conditionally, said claim field including an expression identifying the resource by a resource name and by at least one of the properties.

33. The computer-readable medium of claim 32, wherein the resource name identifies a resource group.

34. The computer-readable medium of claim 32, wherein the validation information further includes a site identifier identifying an application program associated with the user.

35. The computer-readable medium of claim 32, wherein the validation information further includes a site identifier identifying a computing device associated with the user.